IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 10/789,311	§		
Filed: February 27, 2004	§	Examiner:	Johnson, Carlton
Inventors:	§	Group/Art Unit:	2136
Sheueling Chang Shantz, et al.	§	Atty. Dkt. No:	6000-31500
Title: Method and Apparatus for Implementing Processor Instructions for Accelerating Public-Key Cryptography	§		

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants request review of the final rejection in the above-identified application. Claims 1-67 are pending in the application. Reconsideration of the present case is earnestly requested in light of the following remarks. Applicants note the following **clear errors** in the Examiner's rejections.

Section 102 rejection:

The Examiner rejected claims 1-10, 12-19, 21-29, 32-36, 38-46, 48-60 and 62-67 as being *anticipated* by Gressel et al. (U.S. Patent 6,748,410) (hereinafter "Gressel"). Applicants note the following clear errors in the Examiner's rejection.

Independent claim 1:

1. The Examiner has failed to address each and every limitation of claim 1 in his remarks.

The Examiner quotes the entire text of claim 1 and cites a long list of passages in Gressel as teaching: feedback of a previous operation into next operation; arithmetic operation or instructions; arithmetic structure; multiplication two values, summing two values utilizing partial (i.e., bit operations, any bit length, high order bits, low order bits) results from previous multiplication; adder; carry-save adder; carry-out; register usage; XOR operations; redundant representation of numbers; acceleration, improvements of arithmetic operations; arithmetic operations utilized to generate cryptography key(s); and processor utilization for key generation. The Examiner submits that Gressel discloses all the limitations of claim 1, in its current form, in these passages, but does not relate the teachings of these passages to any of the specific limitations of claim 1. Instead, the Examiner merely points out general references to the elements listed above in the system of Gressel, many of which have nothing to do with the limitations recited in claim 1. For example, the Examiner's remarks as to the teachings of the cited

passages in Gressel do not address the limitations "generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number." Rather, the Examiner submits that Gressel teaches, "multiplication two values, summing two values utilizing parallel (i.e., bit operations, any bit length, high order bits, low order bits) results from previous multiplication." **This is not what is recited in claim 1, nor does it teach the limitations of claim 1.** Applicants note MPEP 707.07(d), which requires that, in an Examiner's Action, the ground of rejection, should be "fully and clearly stated". **Since the rejection of claim 1 has not been fully and clearly stated, Applicants assert that it is improper.**

2. Gressel fails to disclose *feeding back high order bits of a previously executed arithmetic instruction in the public-key cryptography application, generated by the first arithmetic circuit, to a second arithmetic circuit comprising a second plurality of arithmetic structures.*

The Examiner submits that the Gressel prior art discloses the results of a first arithmetic operation used as input to another arithmetic operation. **Applicants again note that this generic reference to "results of a first arithmetic operation used as input to another arithmetic operation" is not what is recited in Applicants' claim, nor does it teach the limitations recited therein.**

3. Gressel fails to disclose *generating a first partial result of a currently executing arithmetic instruction... the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number*.

The Examiner submitted that descriptions in Gressel describing adding a value of "any bit length" and generic references to "high order bits" and "low order bits" teach these limitations, citing column 2, lines 31-37. However, this passage describes nothing about "high order bits" or "low order bits" as suggested by the Examiner, or about values representing a partial result of a currently executing arithmetic instruction. **Furthermore, a cited description of multiplying (input) values of any bit length to obtain products and then adding the products together clearly does not teach the specific limitations of the first partial result recited claim 1, i.e., *the first partial result representing the high order bits summed with low order bits of a result of a first number multiplied by a second number*.** In the Response to Arguments section of the Final Action, the Examiner submits, "A bit value of an arbitrary length is a partial result. The high order bits are a partial result. The low order bits are a partial result. The two partial results are combined by adding the products. This is equivalent to a first partial result representing the high order bits summed with the low order bits of a result of a first number multiplied by a second number." **Applicants assert that this interpretation is completely unsupported by the cited**

art. The Examiner's citation merely describes multiplying "integers" of any bit length. As previously noted, nothing in Gressel describes combining "high order bits" and "low order bits", as the Examiner suggests, or a partial result of a currently executing arithmetic instruction, **much less the specific limitations recited in claim 1.** Applicants note that additional cited passages describe multiplication of integers (without any reference to utilizing partial results of a previous operation), and general references to linear feedback shift registers. **None of the cited passages teach the specific limitations of claim 1.** In the Advisory Action, the Examiner submits, "In addition, the Stribaek prior art discloses the selection of high order bits and/or low order bits in arithmetic operations." **Applicants assert that this generic description also does not teach Applicants' claimed invention, and note that the Examiner has improperly included a reference to the Stribaek prior art, even though claim 1 was rejected as being anticipated by Gressel.**

4. Gressel fails to disclose *storing the first partial result; and using the stored first partial result in a subsequent computation in the public-key cryptography application.*

The Examiner submits that Gressel teaches "storing and utilizing the results of an operation in subsequent arithmetic operations" in the passages cited above and in a generic reference to destination addresses of instructions. This teaches nothing about the specific limitations recited in claim 1 regarding a method that includes storing a first partial result (i.e., one having the limitations recited in claim 1) and using this stored first partial result in a subsequent computation in a public-key cryptography application.

5. The Examiner is improperly ignoring the specific wording of Applicants' claims.

In the Response to Arguments section of the Final Action, the Examiner submits, "The claim limitations merely recite arithmetic operations which are performed on integer values. The Gressel and Stribaek prior art combination discloses arithmetic operations performed on integer values. The stated types of operations indicated by the prior art discloses". As discussed above, Applicants' claims do not "merely recite arithmetic operations which are performed on integer values" as erroneously suggested by the Examiner. Instead, claim 1, for example, recites specific operations performed by various *arithmetic circuits of a device* to implement a portion of a *cryptography application*. Applicants remind the Examiner that "All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP 2143.03; *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

6. Gressel fails to disclose all the limitations of claim 1, as arranged in the claim.

Applicants again assert that the Examiner has merely picked and chosen individual disparate words, phrases, and elements of Applicants' claim that are found, or in some cases are not found, in the

Gressel reference and attempted to piece them together in a manner not described in the cited art to reconstruct Applicants' claim. Applicants remind the Examiner that "It is impermissible. . .simply to engage in a hindsight reconstruction of the claimed invention, using the applicant's structure as a template and selecting elements from references to fill the gaps." *In re Gorman*, 933 F.2d 982, 987 (Fed. Cir. 1991). Therefore, Gressel cannot be said to anticipate claim 1. For at least the reasons above, the rejection of claim 1 is unsupported by the prior art and removal thereof is respectfully requested. Similar remarks apply to independent claims 16 and 29, which recite similar limitations and which were rejected using remarks identical to those used in the rejection of claim 1.

Independent claim 21:

1. The Examiner has failed to address each and every limitation of claim 21 in his remarks.

The Examiner again quotes the entire text of claim 21 and cites the same long list of passages in Gressel, including the same remarks used to reject claim 1. Therefore, the arguments presented above apply with equal force to this claim, as well.

2. Gressel fails to disclose *supplying a third number to the second arithmetic circuit; the second arithmetic circuit generating a first partial result of a currently executing arithmetic instruction in the public-key cryptography application, the first partial result being a representation of the high order bits summed with low order bits of a result of a first number multiplied by a second number and with the third number*.

These limitations differ from those in claim 1 and the Examiner has repeatedly failed to specifically address these differences in his remarks. **Therefore, the rejection of claim 21 is improper. Applicants again assert that the Examiner has cited nothing in cited art to teach these limitations, and that it does not teach these limitations.** Therefore, Gressel cannot be said to anticipate claim 21. For at least the reasons above, the rejection of claim 21 is unsupported by the cited art and removal thereof is respectfully requested. Independent claims 53 and 67 include limitations similar to those of claim 21, and were rejected using remarks identical to those used in the rejection of claim 21. Therefore, the arguments presented above apply with equal force to these claims as well.

Section 101 rejection:

The Examiner rejected claims 1-67 under 35 U.S.C. § 101 as being directed to non-statutory matter. In spite of the amendments made to many of the claims in Applicants' Response of September 19, 2007, the Examiner merely repeats his assertion that the claimed invention is based on non-statutory matter and directed towards nothing more than the abstract idea of a mathematical algorithm. Applicants

again traverse this rejection for at least the reasons presented in the Response of January 28, 2007. For example, Applicants note that claims 1 and 21 recite a method implemented in a device supporting a public-key cryptography application, wherein the device comprises multiple arithmetic *circuits* that perform various operations of the method, and to recite limitations involving the storage and subsequent use of a generated partial result in a public-key cryptography application. Applicants assert that none of Applicants' claims consist solely of mathematical operations without some claimed practical application, nor are the mathematical operations recited therein performed in the abstract. Rather, they are performed within a very specific practical context, i.e., in methods, processors, and apparatus supporting public-key cryptography applications. For example, methods implemented in a device supporting public-key cryptography that produce a generated partial result for use in a cryptography application are clearly directed to a claimed practical application. Similarly, processors (such as those of claims 38 and 53) that include structures for implementing various operations of a cryptography application are clearly not directed solely to mathematical operations, but are directed to real-world implementations that support a claimed practical application. In addition, an apparatus configured to support a public-key cryptography application (as in claims 66 and 67) is clearly directed to a real-world implementation of acts performed within a specific practical application. Applicants also note that **none of the claims of the present invention recite merely *a computer program product*,** as erroneously suggested by the Examiner. For at least the reasons above, Applicants respectfully request removal of the rejection of claims 1-67 under 35 U.S.C. § 101.

In light of the foregoing remarks, Applicants submit the application is in condition for allowance, and notice to that effect is respectfully requested. If any extension of time (under 37 C.F.R. § 1.136) is necessary to prevent the above referenced application from becoming abandoned, Applicants hereby petition for such an extension. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert & Goetzel PC Deposit Account No. 501505/6000-31500/RCK.

Respectfully submitted,
/Robert C. Kowert/
Robert C. Kowert, Reg. #39,255
Attorney for Applicants

Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8850

Date: February 28, 2008